IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Gregory Alan Flurry, Bill Lawton, Stewart Earle Nickolas		
Assignee:	International Business Machines Corporation		
Title:	Method and System for Single-Sign-On Mechanism within Application Service Provider (ASP) Aggregation		
Serial No.:	09/965,736	Filing Date:	September 27, 2001
Examiner:	Minh Dinh	Group Art Unit:	2132
Docket No.:	AUS920010571US1	Customer No.	65362

Austin, Texas
December 6, 2007

COMMISSIONER FOR PATENTS
PO BOX 1450
ALEXANDRIA, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

AND STATEMENT OF REASONS

Sir:

Applicants request review of the Final Office Action in this application. No amendments are being filed with the request. This request is being filed with a Notice of Appeal. The following sets forth a succinct, concise, and focused set of arguments for which the review is being requested.

CLAIM STATUS

In the Final Office Action, claims 1, 3, 16, 18 and 31 were rejected under 35 U.S.C. §102(a) as being anticipated by Mishra et al. "Security Services Markup Language" ("Mishra"). Claims 2, 4-5, 17, 19, 20 and 32-34 were rejected under 35 U.S.C. §103(a) as being unpatentable over Mishra as applied to claims 1, 16, and 31, and further in view of U.S. Patent No. 6,226,752 to Gupta et al. ("Gupta"). Claims 6-8, 10-15, 21-23, 25-30, and 35-38 are rejected under 35 U.S.C. §103(a) as being unpatentable over Mishra in view of Gupta. Claims 9 and 24 are rejected under 35 U.S.C. §103(a) as being unpatentable over Mishra in view of Gupta as applied

to claims 6 and 21, and further in view of U.S. Publication No. 2002/0029269 to McCarty et al. ("McCarty").

Applicants' invention relates to a method, system, apparatus, or computer program product for providing a single-sign-on mechanism within an ASP aggregator service. Each of the independent claims 1, 6, 16, 18 and 31 recite the limitation of an aggregator token that is generated by an ASP aggregator service and sent to a client device after its user has been successfully authenticated during a single-sign-on operation that is provided by the ASP aggregator service. The aggregator token then accompanies any request from the client to aggregated applications within the ASP aggregator service's infrastructure. In various embodiments of the invention, the aggregator token comprises an indication of an address or resource identifier within the ASP aggregator service to which a client/user can be redirected when the client/user needs to be authenticated by the ASP aggregator service.

For convenience, Examiner's response to Applicants' prior remarks is set forth below:

> Applicant argues that Mishra does not teach the use of an aggregator token (see Remark, page 10, 3rd paragraph), wherein (i) the aggregator token is generated and sent to a client after its user has been successfully authenticated during a single-sign-on operation that is provided by the ASP aggregator service; (ii) the aggregator token then accompanies any request from the client to aggregated applications within the ASP aggregator service's infrastructure; and (iii) in various embodiments of the invention, the aggregator token comprises an indication of an address or resource identifier within the ASP aggregator service to which a client/user can be redirected when the client/user needs to be authenticated by the ASP aggregator service (see Remark, page 10, 2nd paragraph).
>
> Mishra, et al ("Security Services Markup Language") discloses that an aggregator token, i.e., a name assertion, is generated and sent to an client as part of an authentication response message after its user has been successfully authenticated during a single-sign-on operation that is provided by the ASP aggregator service (page 4, definition of a Name Assertion; pages 7-8, Section 3.1, Scenario #1; User-Driven Transactions (Single Sign-On); page 16, AuthResponse message).
>
> Mishra also discloses that the aggregator token then accompanies a request from the client to an aggregated application within the ASP aggregator service's infrastructure, i.e., the Name Assertion is included in the user's request to access site B (pages 7-8), Section 3.1, Scenario #1: User-Driven Transactions (Single Sign-On)).
>
> With respect to independent claims 1, 16 and 31, Mishra further discloses that the aggregator token comprises a logon resource identifier, i.e., the URI of the authentication engine which authenticates the user and issues aggregator token (page 12 and 16, see the <Issuer> tag within the <NameAssertion> of the authentication response from the authentication engine).

Mishra teaches that a Security Services Markup Language (S2ML) Name Assertion is generated and sent to a client as part of an authentication response message after its user has been successfully authenticated during a single sign-on (SSO) operation. As such, an S2ML Name Assertion comprises the identification of the authentication Issuer (page 12 and 16, see the

<Issuer> tag within the <NameAssertion> of the authentication response from the authentication engine).

The "aggregator token," as described in Applicants' disclosure, is "returned to the client/user by the ASP aggregator service in response to successful, initial, authentication operation" (paragraph 0067). However, the aggregator token comprises "an address that indicates the logon resource to which a user should be redirected if an ASP, aggregated application, or other entity in the ASP aggregator service's infrastructure determines that the user has not been properly authenticated when processing a request from the user for access to a resource that is supported or protected by the entity that received the request" (paragraph 0073). The address within the aggregator token "identifies a logon application, a logon start page, or similar logon resource (paragraph 0067).

While an S2ML Name Assertion and an aggregator token of Applicants' invention are both generated as a result of a successful authentication operation, they provide different functionalities. The URI or URL address of an S2ML Name Assertion provides the identity of the Authenticator, whereas the URI or URL address of an Aggregator token provides the location of a logon page associated with the Authenticator. Similarly, both the Name Assertion and the aggregator token are conveyed by the user's client from one ASP site to another. The Name Assertion provides the identity of the Authenticator to each ASP site, and assuming that its associated entitlements are still valid, re-authentication of the user is not required. However, if the user attempts to use information from a prior session (e.g., the URL of a previously-visited ASP, or a Name Assertion with expired entitlements), the aggregator token provides the address of logon resource for re-authentication of the user. As a result, the user is automatically redirected to the logon resource without having to re-enter the address of the logon resource, even if the Entitlement associated with the Name Assertion has expired.

Examiner's comment regarding other independent claims:

> With respect to the other independent claims, whereas Mishra discloses using the logon resource identifier to request the logon resource for further information regarding the authenticated user (page 8), Mishra does not disclose using the logon resource identifier for the purpose of redirecting users who need to be authenticated; however, this feature is taught by Gupta et al (6,226,752).

Mishra discloses using a portable S2ML Name Assertion, comprising authentication type, subject name and Authenticator (page 4) that can be conveyed from a first ASP site to a second ASP site (page 8). The Entitlement, which is an assertion comprising authorization data,

is similarly generated by the Authenticator and is likewise portable from a first ASP site to a second ASP site (page 8). However, neither the S2ML Name Assertion nor the Entitlement comprise the logon resource identifier of the invention, which is not used to identify the Authenticator that issues the Name Assertion or its associated Entitlement. Instead, the logon resource identifier contained in the aggregator token is used to redirect the user to a logon resource without having to re-enter the address of the logon resource, even if the Entitlement associated with the Name Assertion has expired.

Gupta teaches that an authentication cookie (or token) is generated by an authentication server, which is then conveyed to the user's client. The client then submits the authentication cookie (or token) to a first target application server and is provided access. If the user then attempts to access a second target application server, the cookie stored in user's client is then submitted back to the authentication server that issued it. The authentication server, recognizing the authentication cookie (or token) that it previously generated, does not require the user to be re-authenticated. As a result, the user is automatically re-authenticated for access to the second target application server (column 12, lines 50-60). It will be appreciated that the approach taught by Gupta requires the client to submit a previously-generated authentication cookie to the authenticator that generated it each time a different application server is accessed. Conversely, the logon resource of the invention is conveyed from one ASP site to another and is only used when the Entitlement associated with a Name Assertion has expired and the user needs to be re-authenticated by the ASP aggregator Authenticator.

Independent claims 13, 21, 28, 35, and 38 each recite an aggregator token as a limitation and, therefore, the arguments submitted herein regarding the aggregator token of Applicants' invention apply with equal force to the allowability of these independent claims.

For the reasons set forth above, Applicants respectfully submit that the rejection of independent claims 1, 6, 13, 16, 18, 21, 35, 31, 35 and 38 under 35 U.S.C. §102 and/or §103 is improper and should be removed. Furthermore, all of the pending dependent claims are allowable since they are dependent on allowable base claims.

CONCLUSION

In view of the remarks set forth herein, the application is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned at 512-338-9100.

FILED ELECTRONICALLY
December 6, 2007

Respectfully submitted,

/Gary W. Hamilton/

Gary W. Hamilton
Attorney for Applicants
Reg. No. 31,834